Distributed Denial of Service (DDoS)

If a DDoS attack occurs, what is the cost to your business?

Denial of Service (DoS) attacks in various forms have existed for decades and yet they are still grabbing the headlines. The first high profile examples of Distributed Denial of Service (DDoS) attacks on global companies such as Amazon, Buy.com and EBay were reported in February 2000. There was the usual angst around loss of service availability and a dramatic impact on sales and revenue – and then we moved on. These were internet businesses after all.

Now, over a decade later, we all rely on the internet to do business, even taking availability for granted – and according to the companies surveyed in Arbor Networks’ ninth annual Worldwide Infrastructure Security Report, DDoS attacks against infrastructure top the list of security concerns for 2014. So why is DDoS suddenly so high on our profession’s list of concerns? Perhaps it is the apparent escalation in the number of attacks on data centers and mobile networks, or maybe the frequency of incidents – up 50% and 100% respectively, according to Arbor’s report. But heightened awareness does not mean that DDoS is being given the necessary focus and investment – despite the very real impact it is having on organizations all over the world. Our Global Threat Intelligence Report\(^1\) highlights that DDoS attacks accounted for 31% of incident response engagements in 2013. The facts show that the cost of DDoS should not only be judged in terms of lost potential revenue and availability of systems - which for some organizations can be counted in thousands of dollars per second - but also in escalating remediation costs.

In our experience, most organizations fail to realize the potential impact of a DDoS attack, which is why many are still not budgeting for and implementing proactive controls, or planning the right mitigation and incident response. When you are under a DDoS attack, scrambling for budget, purchasing solutions and obtaining approval to implement controls, at the same time as desperately attempting to understand the threat and restore systems, the result will almost certainly be higher, less effective spend.

How have DDoS attacks developed and what are the implications for existing information security architectures and controls?

Denial of service or Distributed Denial of Service attacks typically aim to disrupt or totally block an organization’s web services.

To ensure that investment in DDoS protection and response evolves ahead of the threat, organizations must:

1. Recognize how DDoS attacks have developed and the implications for existing information security architectures and controls
2. Understand the options to maximize the value of offensive security processes and technology
3. Implement the right incident response model for your business

The result – your customers, employees and partners can no longer access business critical web applications, all online transactions stop, visibility of your people and assets goes dark. The motivation for these attacks varies from criminal intent to malicious mischief – as disruptive elements seek to publicly embarrass their target. And their scope is widening. Initially DDoS attacks focused on ecommerce, egaming and finance platforms but have now been seen targeting all businesses with an online presence.

Traditional motivators for DDoS attacks – such as hactivism, extortion and cybercrime – are

---

\(^1\) NTT Group Global Threat Intelligence Report, 2014. For more information and to download the report, please visit: www.nttcomsecurity.com/gtir
now being joined by the risk to competitive advantage if a competitor’s site is available and yours is not. If your industry sector is being specifically hit by DDoS attacks and you avert an incident – you have the advantage of maintaining business and your reputation. An example of this was when in 2012; several major US banks suffered a DDoS attack simultaneously. Those that had invested in the right DDoS protection not only maintained business, but also saw a flight of customers from other affected banks. Consumer expectations of availability mean that any loss of service could also mean loss of custom.

So what is DDoS?
DDoS is typically seen as a volumetric attack which consumes all the resource that your Wide Area Network (WAN) connection, firewall and/or web servers can support. However, a more sinister side to DDoS is emerging, with criminal factions using denial of service as a diversionary tactic – distracting information security focus and resources whilst they execute sophisticated Advanced Persistent Threat (APT) attacks to steal data or intellectual property. But whatever the motivation, loss of web availability impacts the confidence of investors, customers and employees.

To manage DDoS effectively, you must recognize it when it happens – and the reality is, it may not be obvious to a network or system administrator that the company’s infrastructure is under attack. When they receive the initial alert highlighting a network slowdown, often the natural assumption is that there is a technical problem or traffic congestion. DDoS attacks usually have a build-up stage, and it may only be as the attack progresses and starts to seriously impact availability, that it will be diagnosed.

So how do we categorize these attacks?

Volumetric attacks
These attacks can often be tracked back to botnets or vulnerable networks. They are high bandwidth and geographically diverse. Volumetric attacks often result in some sort of collateral damage as devices such as routers, firewalls or load balancers become overloaded and the network hosting the target becomes inaccessible.

> **TCP SYN Flood:** An attacker makes connection requests aimed at the victim’s server with packets with unreachable source addresses. This results in the victim wasting all of its network resources
> **UDP Flood:** UDP is cheap and easy to generate
> **ICMP Flood:** Is easy and cheap to generate. These attacks are not as common because network operators are putting in measures to limit or block this type of attack
> **Reflection Attack:** These attacks have become more popular as the true source of the attack is difficult to find (it does not require a botnet) and can easily be amplified

Application Layer attacks
Application layer attacks are well-crafted – targeting a specific service on the host. These attacks can be difficult to detect as they initially appear to be a legitimate connection but are often filled with garbage requests. They are also popular due to the numerous tools available, including:

> **HTTP-GET Attack:** HTTP-GET attacks are designed to use up resources on web servers and look like a legitimate request
> **HTTP-POST attack:** These attacks operate in a similar way to HTTP-GET attacks except they make a POST to the servicer instead of a GET request
> **SSL Attacks:** As most services move to SSL encryption, we see attacks against SSL are on the increase globally

Application layer traffic visibility and control are key elements of creating a layered DDoS defence. Network layer solutions that evolved to combat volumetric attacks are blind to application layer attacks – without the deep insight of application protocols or the ability to terminate and actively seize control of the application sessions and sanitize them.

The implication of DDoS attacks on existing infrastructure and controls
DDoS protection is not an insignificant investment, so it is worth taking some time to make the right decision for your business. In some respects, DDoS protection requires a change in your organization’s mindset as to how an online service is deployed and delivered. There are a number of pitfalls that you can easily fall into and the management of a DDoS solution is something that definitely needs time to get embedded into any infrastructure. Your investment will also be wasted if you don’t invest in the right processes to get the most from that solution. The big mistake is to focus on the technology that DDoS protection provides, rather than what you want it to protect. Where DDoS deployment often goes wrong is around planning and executing how to get your services and applications behind the DDoS solution.

But what is certain is that turning on the DDoS protection on your Unified Threat Manager (UTM) / next generation firewall, will still fail to protect you from most attacks. The fact is that dealing with a volumetric attack requires a lot of computing resource that your firewall cannot provide. So let’s look at what options you have to protect your organization.

Maximize the value of offensive security processes and technology
There are a number of different approaches to DDoS mitigation. DDoS attacks can be mitigated through the use on-premise inline devices, cloud-based scrubbing solutions or a careful combination of these two technologies.

Intelligence shows that commercial customers are the most common target of volumetric attacks. These attacks, as we have discussed, are quick, easy and cheap to run and are commonly above 1Gbps in size. This means when choosing the right solution, organizations must be able to mitigate large volumes of traffic that would ordinarily swamp their ISP connection. In our view based on the global developments in DDoS attacks, a hybrid approach provides the most robust, cost-effective solution – providing the confidence that your investment will allow you to manage any incident, whatever the scale, at a predictable, budgeted cost.
1. On-premise device protects against application layer attacks signalling to the cloud if a volumetric attack is detected

2. Cloud-based protection steps inline during volumetric attacks, scrubbing data to allow sanitized business traffic to pass

Implement the right incident response model for your business

So what happens when you are attacked? To answer this question, the business must consider the strategy for incident response. How to react to and manage a DDoS attack will be a key part of this plan.

In an ideal world, investing in a DDoS solution would protect you from ever suffering an attack. In practice, 100% protection is very difficult to do and attackers find new ways to interrupt a service all the time, motivated by a wide range of economic, political and commercial factors. But what an effective DDoS solution will give you is the monitoring capability to react quickly to an attack. Couple this with strong, mature incident management and you can neutralize the noise and commercial impact of an attack.

Preparing to manage a security incident, organizations should:

> Think more about process and people - mature incident response does not necessarily mean spending more on technology

> Think through your approach to what you’re protecting - good incident response starts with good risk insight and understanding of your information assets

> Consider the value of using high visibility exercises, simulating potential incidents to improve awareness and define roles and responsibilities beyond the technology teams

> Establish what skills you already have, what you would need if you were breached and where to go for help in the event of an incident

> Understand where compliance fits into your incident response processes and have a clear procedure in place to meet your specific obligations for reporting incidents

Case studies:

How our customer maximized an investment in DDoS mitigation

A global customer was suffering a DDoS attack, on a service that was key for the business. The company was being threatened with blackmail and approached NTT Com Security for emergency advice and assistance to mitigate what could have been a catastrophic attack for the business.

The business value of the right DDoS mitigation solution

> A DDoS solution was put in place quickly to minimize the impact to business as usual

> Then the customer refused to pay the blackmail and the attackers tried to bring down the site, the solution delivered critical support which stopped the attack having serious consequences to their business

> The company is now in a position to get ahead of potential attacks and proactively manage risk
Conclusion

Today’s businesses cannot afford a service being unavailable for days whilst a mitigation plan is formulated and actioned. The need to get DDoS right first time and the complexities of doing so is why our customers often involve us early in identifying the risk of DDoS to find the right solution as well as the technical installation and configuration. DDoS is not a new problem, but we see new forms of this kind of attack constantly evolving. Businesses must look at this within the strategic information security approach, defined policies, service levels and risk posture to ensure that any solution is correctly aligned to deliver the right proactive and remedial action.

Understanding the value of information assets: how a proportionate response to DDoS helped our customer achieve the right level of protection

An NTT Com Security customer had selected a DDoS vendor but was unsure about how, within the multinational organization, the right level of protection should be deployed to individual assets and services. The company approached NTT Com Security for help understanding and defining the process by which stakeholders could scope and achieve the right level of protection for each system.

The business value of the right DDoS protection and incident response strategy

> NTT Com Security helped the customer articulate the right incident response with business goals and requirements front and center

> Clarifying and communicating the opt-in/opt-out criteria helped system owners understand their roles and responsibilities and how they should engage with the centralized DDoS system

> The customer increased the maturity of their incident response planning and execution, as well as simplifying the scope of the DDoS solution, to make sure the right levels of protection were achieved

We see a more secure world

NTT Com Security is in the business of information security and risk management. By choosing our WideAngle consulting, managed security and technology services, our customers are free to focus on business opportunities while we focus on managing risk.

The breadth of our Governance, Risk and Compliance (GRC) engagements, innovative managed security services and pragmatic technology implementations, means we can share a unique perspective with our customers – helping them to prioritize projects and drive standards. We want to give the right objective advice every time.

Our global approach is designed to drive out cost and complexity – recognizing the growing value of information security and risk management as a differentiator in high-performing businesses. Innovative and independent, NTT Com Security (formerly Integralis), has offices spanning the Americas, Europe, and APAC (Asia Pacific) and is part of the NTT Communications Group, owned by NTT (Nippon Telegraph and Telephone Corporation), one of the largest telecommunications companies in the world.

To learn more about NTT Com Security and our unique WideAngle services for information security and risk management, please speak to your account representative or visit: www.nttcomsecurity.com for regional contact information.